

What Is Claimed Is:

1. A method for confirming communication of data to a first device belonging to a first user from a second device belonging to a second user, the method comprising:
 - receiving a message containing data from the second device at the first
5 device;
 - translating the data into a string of words that can be recognized by a human;
 - allowing the second device to translate the data into a corresponding string of words;
 - 10 displaying the string of words to the first user; and
 - allowing the first user and the second user to confirm a match between the string of words from the first device and the corresponding string of words from the second device, wherein the confirmation process is performed through a separate communication channel, and wherein the confirmation ensures that the
15 data sent by the second device is successfully received by the first device, is authentic, and is integrity-checked.
2. The method of claim 1, wherein prior to receiving the message, the first device broadcasts a request asking for the second device's data, and wherein the data can be an identifier.
3. The method of claim 1,
 - wherein the message received by the first device is signed with a private key corresponding to a public key associated with the second device; and
 - wherein the method further comprises using the public key associated with
5 the second device to verify that the message is signed with the private key associated with the second device.

4. The method of claim 1,
wherein while receiving the message, the first device receives more than
one message; and

5 wherein the method further comprises translating the data in the other
messages into strings of words which can be recognized by a human, and
displaying these strings of words to the first user, thereby allowing the first user to
match one of these strings of words with the corresponding string derived by the
second device from the original data.

5 5. The method of claim 1, wherein prior to the reception of the
message at the first device, the first user obtains a portion of the hash of the data
on a separate communication channel and enters this portion into the first device,
and wherein the first device uses this portion to filter subsequently received
messages.

6. The method of claim 1, wherein the data received at the first device
contains a cryptographically generated address (CGA) belonging to the second
device, which is generated by:
performing a hash function on the second device's public key; and
5 constructing the CGA by combining a number of bits of an address
belonging to the second device and a number of bits from the result of the hash
function.

7. The method of claim 6,
wherein the message received by the first device includes a public key
associated with the sending device; and
wherein the method further comprises performing a hash function on the
5 public key to verify the association between the received CGA and the public key
associated with the sending device.

8. The method of claim 1, wherein the translation uses a one-time password (OTP) dictionary.

9. The method of claim 2,
wherein the request includes a CBID belonging to the first device; and
wherein the request is signed with a private key associated with the first device, thereby allowing the request to be verifiably associated with the first
5 device.

10. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for confirming communication of data to a first device belonging to a first user from a second device belonging to a second user, the method comprising:
5 receiving a message containing data from the second device at the first device;
translating the data into a string of words that can be recognized by a human;
allowing the second device to translate the data into a corresponding string
10 of words;
displaying the string of words to the first user; and
allowing the first user and the second user to confirm a match between the string of words from the first device and the corresponding string of words from the second device, wherein the confirmation process is performed through a
15 separate communication channel, and wherein the confirmation ensures that the data sent by the second device is successfully received by the first device, is authentic, and is integrity-checked.

11. The computer-readable storage medium of claim 10, wherein prior to receiving the message, wherein prior to receiving the message, the first device

broadcasts a request asking for the second device's data, and wherein the data can be an identifier.

5

12. The computer-readable storage medium of claim 10,
wherein the message received by the first device is signed with a private
key corresponding to a public key associated with the second device; and
wherein the method further comprises using the public key associated with
5 the second device to verify that the message is signed with the private key
associated with the second device.

13. The computer-readable storage medium of claim 10,
wherein while receiving the message, the first device receives more than
one message; and

wherein the method further comprises translating the data in the other
5 messages into strings of words which can be recognized by a human, and
displaying these strings of words to the first user, thereby allowing the first user to
match one of these strings of words with the corresponding string derived by the
second device from the original data.

14. The computer-readable storage medium of claim 10, wherein prior
to the reception of the message at the first device, the first user obtains a portion
of the hash of the data on a separate communication channel and enters this
portion into the first device, and wherein the first device uses this portion to filter
5 subsequently received messages.

15. The computer-readable storage medium of claim 10, wherein the
data received at the first device contains a cryptographically generated address
(CGA) belonging to the second device, which is generated by:
performing a hash function on the second device's public key; and

5 constructing the CGA by combining a number of bits of an address
belonging to the second device and a number of bits from the result of the hash
function.

16. The computer-readable storage medium of claim 15,
wherein the message received by the first device includes a public key
associated with the sending device; and
wherein the method further comprises performing a hash function on the
5 public key to verify the association between the received CGA and the public key
associated with the sending device.

17. The computer-readable storage medium of claim 10, wherein the
translation uses a one-time password (OTP) dictionary.

18. The method of claim 11,
wherein the request includes a CBID belonging to the first device; and
wherein the request is signed with a private key associated with the first
device, thereby allowing the request to be verifiably associated with the first
5 device.

19. An apparatus that confirms communication of data between a first
user and a second user, comprising:
a receiving mechanism in a first device belonging to the first user, the
receiving mechanism configured to receive a message containing data from a
5 second device belonging to the second user;
a translation mechanism in the first device configured to translate the data
into a string of words that can be recognized by a human;
a display mechanism configured to display the string of words to the first
user; and

10 a confirmation mechanism that allows the first user and the second user to
confirm a match between the string of words from the first device and a
corresponding string of words translated from the data at the second device,
wherein the confirmation process is performed through a separate communication
channel, and wherein the confirmation ensures that the data sent by the second
15 device is successfully received by the first device, is authentic, and is integrity-
checked.

20. The apparatus of claim 19, wherein prior to receiving the message,
the first device is configured to broadcast a request asking for the second device's
data, and wherein the data can be an identifier.

21. The apparatus of claim 19,
wherein the message received by the first device is signed with a private
key corresponding to a public key associated with the second device; and
wherein the apparatus further comprises a verification mechanism
5 configured to use the public key associated with the second device to verify that
the message is signed with the private key associated with the second device.

22. The apparatus of claim 19,
wherein the first device is configured to receive more than one message
while receiving the message;
wherein the translation mechanism is further configured to translate the
5 data in the other messages into strings of words which can be recognized by a
human; and
wherein the display mechanism is further configured to display these
strings of words to the first user, thereby allowing the first user to match these
string of words with the corresponding string derived by the second device from
10 the original data.

23. The apparatus of claim 19, wherein prior to the reception of the message at the first device, the first device is configured to enable the first user to obtain a portion of the hash of the data on a separate communication channel and to enter this portion into the first device, and wherein the first device is configured
5 to use this portion to filter subsequently received messages.

24. The apparatus of claim 19, wherein the data received at the first device contains a cryptographically generated address (CGA) belonging to the second device, which is generated by:
performing a hash function on the second device's public key; and
5 constructing the CGA by combining a number of bits of an address belonging to the second device and a number of bits from the result of the hash function.

25. The apparatus of claim 24,
wherein the message received by the first device includes a public key associated with the sending device; and
wherein the apparatus further comprises a verification mechanism
5 configured to perform a hash function on the public key to verify the association between the received CGA and the public key associated with the sending device.

26. The apparatus of claim 19, wherein the translation mechanism uses a one-time password (OTP) dictionary.

27. The apparatus of claim 20,
wherein the request includes a CBID belonging to the first device; and
wherein the request is signed with a private key associated with the first device, thereby allowing the request to be verifiably associated with the first
5 device.